Diretrizes de Hardening

Santos Bevilaqua Advogados

Sumário

1. Introdução

Hardening é o processo de aprimorar a segurança de uma infraestrutura para resistir a ataques. Ele abrange desde a identificação de vulnerabilidades e o mapeamento de ameaças até a implementação de ações para mitigar ou minimizar riscos e a execução de atividades corretivas.

Esse procedimento de segurança inclui diversas práticas, como:

- ⇒ Autenticação de usuários e controle de suas autorizações de acesso.
- ⇒ Manutenção de registros (logs) para futuras auditorias.
- ⇒ Sincronização de relógios para garantir a consistência dos dados.
- ⇒ Aplicação de técnicas seguras de acesso à infraestrutura.

Além dessas medidas, o Hardening também envolve a manutenção de registros das operações, o cuidado com as características do sistema (como a atualização constante de softwares), a garantia de que apenas recursos essenciais estejam ativos, e o cumprimento de requisitos de configuração, como a manutenção de backups.

É fundamental ressaltar que a não conformidade com essas diretrizes pode impactar significativamente a eficiência do escritório. Por isso, todos os colaboradores, independentemente de sua posição hierárquica, têm a obrigação de seguir as orientações apresentadas neste documento.

O Santos Bevilaqua Advogados formaliza o compromisso da organização com a proteção de seus ativos de informação, sejam eles de sua propriedade ou sob sua guarda.

O objetivo primordial das diretrizes é estabelecer estratégicas para a manutenção da Segurança da Informação e Comunicações. Visa-se, assim, assegurar a confidencialidade, integridade, disponibilidade e autenticidade dos dados e informações. Isso engloba todos os dados e informações que são produzidos, adquiridos, armazenados, em trânsito, descartados, de propriedade ou sob controle ou operação dos sistemas do Santos Bevilaqua Advogados.

2. Abrangência

É obrigatório seguir esta norma em todas as dependências físicas do Santos Bevilaqua Advogados, que incluem

⇒ Sede

⇒ Unidades regionais

⇒ Centros de processamento

⇒ Quaisquer outros locais pertencentes ao patrimônio ou sob a custódia do Santos Bevilaqua Advogados.

2.1. Ativos e Ambientes Computacionais Cobertos

As diretrizes de hardening também incide sobre todos os ambientes computacionais e ativos de informação que pertencem ou são custodiados pelo Santos Bevilaqua Advogados. Isso inclui, mas não se limita a:

⇒ Computadores

⇒ Roteadores e switches

⇒ Servidores

⇒ Bancos de dados

⇒ Sistemas de armazenamento

⇒ Redes de comunicação

⇒ Aplicações e softwares em geral.

2.2.Responsabilidades dos Colaboradores

Todos os empregados, colaboradores de qualquer natureza do Santos Bevilaqua Advogados compreendam integralmente e sigam as diretrizes estabelecidas. A adesão a estas normas é crucial para a segurança da informação da empresa.

2.3. Alterações em Sistemas e Aplicações

Qualquer alteração ou modificação em sistemas e aplicações do Santos Bevilaqua Advogados deve seguir rigorosamente as normas e procedimentos internos estabelecidos para gestão de mudanças, garantindo a integridade e a segurança dos ambientes.

3. Referências Normativas

Normas técnicas da ABNT: Conjunto de normas que estabelecem padrões e requisitos para diversos aspectos da segurança da informação, como a NBR ISO/IEC 27002:2022, que trata do sistema de gestão de segurança da informação.

https://www.abntcatalogo.com.br/pnm.aspx?Q=T2JVQ1FZQkZsejNJL1QvVEhmcXlZTUdITWczYm9IZGhGOFNhcnc0WlVDbz0=

4. Procedimentos de Hardening

4.1. Autenticação

A autenticação é o processo de verificar a identidade de um usuário ao tentar acessar os sistemas. Conforme a norma ABNT NBR ISO/IEC 27000, é a garantia de que a identidade de uma entidade é verdadeira.

No Santos Bevilaqua Advogados, os requisitos básicos para autenticação de usuários incluem:

- ⇒ Criar um usuário individual para cada operador ativo, desativando contas antigas.
- ⇒ Evitar que uma única conta de administração padrão seja compartilhada entre diferentes usuários.
- ⇒ Exigir o uso de senhas fortes.
- ⇒ Proibir o armazenamento de senhas em texto puro (não criptografado).
- ⇒ Utilizar o duplo fator de autenticação (MFA) para uma camada extra de segurança.

4.2.Autorização

A autorização define os privilégios de acesso concedidos aos usuários que já foram autenticados nos sistemas. Ela segue os princípios de "least privilege" (menor privilégio) e "need to know" (necessidade de saber), ou seja, cada usuário só tem acesso ao mínimo necessário para desempenhar suas funções.

Os procedimentos de autorização no Santos Bevilaqua Advogados são:

- Todos os usuários do Sistema Santos Bevilaqua Advogados precisam de permissão para acessar os equipamentos, de acordo com as suas atribuições de trabalho.
- A senha de administrador não deve ser compartilhada com todos os usuários, a fim de prevenir acidentes, ações maliciosas ou o uso por pessoas sem a formação adequada para lidar com esses recursos.
- Dispositivos externos que serão conectados à rede do Santos Bevilaqua Advogados devem ser primeiramente autorizados pelo comitê de Segurança da Informação.
- Os usuários são classificados em grupos de privilégio, uma funcionalidade comum em diversos sistemas, para gerenciar suas permissões de forma eficiente.

4.3.Auditoria

A auditoria envolve o acesso a informações sobre como os usuários utilizam os recursos da infraestrutura.

Os procedimentos básicos de auditoria são:

⇒ Manter um registro detalhado de cada usuário e suas respectivas permissões.

⇒ Registrar todas as ações dos usuários nos sistemas.

⇒ Classificar os registros por nível de criticidade: Informativo, Aviso e Crítico.

⇒ Classificar os registros por tipo: Documentos, Registros (Logs) e Backup de configuração.

⇒ Garantir que todos os registros tenham data e hora corretas.

4.4. Acesso

O acesso aos equipamentos da rede deve ser feito de forma segura, seguindo estes procedimentos básicos:

⇒ Todos os equipamentos serão criptografados.

⇒ Todos os equipamentos têm uma regra de bloqueio automático por tempo de inatividade.

⇒ As permissões de acesso são concedidas conforme as políticas de permissionamento definidas pelos gestores.

⇒ As permissões variam de acordo com a função de cada colaborador.

4.5. Registros

Todos os registros (logs) gerados pela operação e configuração da rede devem seguir estes procedimentos básicos:

⇒ Os registros serão configurados com diferentes níveis de criticidade.

⇒ A data e o horário dos registros são sincronizados com o https://ntp.br/.

4.6. Gestão de Horário dos Servidores

Entendemos que a sincronização de tempo é fundamental porque todas as atividades de gerenciamento, proteção, planejamento e depuração de uma rede dependem da determinação exata de quando os eventos ocorrem. O tempo é o único referencial comum entre todos os dispositivos na rede. Sem a sincronização, é difícil, ou até impossível, correlacionar com precisão os arquivos de log entre esses dispositivos.

Além disso:

⇒ Rastrear violações de segurança, uso da rede ou problemas que afetam muitos componentes pode ser quase impossível se os registros de data e hora nos logs estiverem imprecisos. O tempo é frequentemente o fator crítico que permite mapear um evento em um nó da rede para um evento correspondente em outro.

⇒ Para evitar confusão em sistemas de arquivos compartilhados, é importante que os horários de modificação sejam consistentes, independentemente da máquina onde os arquivos estão.

4.7.Patching

Sistemas Operacionais e muitos softwares contêm programas próprios que podem apresentar falhas de segurança. Para evitar isso, os fornecedores liberam patches de segurança periodicamente, que precisam ser aplicados.

Ignorar essas atualizações podem permitir que um hacker comprometa um computador, ameaçando a integridade da rede do Santos Bevilaqua Advogados e de todos os dispositivos conectados.

O Santos Bevilaqua Advogados utiliza o sistema operacionais Microsoft Windows. Os patches relacionados a esses sistemas, sejam de segurança ou críticos, devem ser instalados o mais rápido possível.

Para gerenciar e priorizar a aplicação de atualizações e correções, os patches de segurança são classificados conforme o sistema de avaliação de severidade da Microsoft, detalhado nas tabelas a seguir:

Classificação	Descrição
Crítico	Máquinas com vulnerabilidades podem se tornar um vetor para a disseminação automática de vírus, sem a necessidade de qualquer interação do usuário.
Importante	Vulnerabilidades que podem levar à perda de confidencialidade, integridade ou disponibilidade dos dados dos usuários, além de afetar a capacidade ou a correção dos recursos de processamento.

Moderado	Correções de segurança cujas vulnerabilidades se tornam substancialmente menos exploráveis através de configurações padrão, auditoria regular ou mecanismos que dificultam a sua ativação.
Baixo	Possuem vulnerabilidades que são extremamente difíceis de explorar ou que, mesmo exploradas, resultam em impacto mínimo.

4.8.Sistema

Todos os novos sistemas devem seguir as seguintes recomendações:

⇒ Instalar conforme as recomendações do fornecedor;

⇒ Desativar as interfaces não utilizadas;

⇒ Desativar serviços não utilizados, inseguros, DNS recursivo e Servidor NTP;

⇒ Remover ou desativar pacotes de funções extras não utilizados;

⇒ Manter o sistema sempre atualizado na versão mais recente e estável;

⇒ Realizar scans de vulnerabilidades e corrigir todas as que forem encontradas.

5. Implementação e Atualização

A Política de Criptografia do Santos Bevilaqua Advogados ser atualizada sempre que necessário.